REMARKS

Claim 54 is copied verbatim from U.S. Patent No. 6,292,569, granted September 18, 2001, to Shear et al. Claim 54 corresponds to Shear's claim 1. In accordance with 37 C.F.R. § 1.607(a), the copied claim may be specifically applied to Applicants' disclosure as follows:

Copied Claim	**Applicants' Disclosure In MEDIDNA.1C1C1**
54. A security method comprising:	Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, ll.17-19).

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

(a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class;	• Applicants disclose encrypting (i.e., digitally signing) control elements and a data object (i.e., a first load module) (p.4, ll.27-28; p.12, ll.15-18) to create a secure data package ready for transfer to a user (p.5, ll.7-10). Applicants disclose that usage control elements define a variety of usages of the data object, for example the kind of user, allowed operations, and security modules required for use of the data object on a user's data processor (i.e., the digital signature designates the load module for use by a device class). (p.4, ll.11-15; p.18, ll.1-5). • Applicants further disclose that the security of a data package can be improved by using a sophisticated encryption algorithm like RSA (p.21, ll.18-20) or other encryption and key methods (p.12, ll.15-18). Such usage is recognized as applying a digital signature. *See e.g.*, Shear '569, col.13, ll.8-10 and 25-26 (Different digital signatures can be made by using different encryption algorithms. Two digital signature algorithms in widespread use today include RSA (a public key cryptosystem) and digital signature algorithm (DSA)). • Applicants disclose that the user's data processor is a general or special purpose processor (p.17, ll.2-3), data objects include books, films, video, news, music, software, games, etc. (p.2, ll.3-4), and the data object owner may want to have control over how, when, where, and by whom his property is used (p.2, ll.20-21). Applicants further disclose that object security is extensible in the sense that multiple levels of security can be applied, being dependent on the encryption/key method which is implemented in the security modules. (p.23, ll.26-29). Thus, Applicants disclose that a variety of data objects (i.e., load modules) can be designated for use by data processors having certain required security modules (i.e., a device class). • Therefore, Applicants disclose digitally signing (i.e., encrypting) a first load module (i.e., a data object such as a digital image or a video file) with a first digital signature designating the first load module for use by a first device class (i.e., the encrypted control/usage elements require the user's data processor to have certain required security modules in order to use the data object).

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

(b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class;	• *See* (a) above regarding digitally signing a load module and designating a device class. • Applicants disclose the secure transfer of two different examples of data objects, a digital image (i.e., a first load module) and a video film (i.e., a second load module), requiring different security treatment with different security modules by a user's data processor prior to usage of the data objects (i.e., designating load modules for use by devices having different tamper resistance and/or work factors). (p.20, l.5-p.23, l.2). • Applicants disclose that the general set of control data associated with a data object comprises an identifier, which uniquely identifies the general set of control data. The whole set of control data and the data object may be encrypted (i.e., digital signature of a second load module can be different from a digital signature of a first load module). (p.4, ll.19-28). • Applicants disclose that a user program comprising a usage manager module controls the usage of a data object in accordance with the control data. The user program comprises one or more security modules (i.e., user device level of security, or user device tamper resistance and/or work factor). (p.17, ll.15-20). The usage manager module applies the security modules which are necessary to use a data object. If the proper security modules are not available for a particular data object, the usage manager module will not permit usage of the data object (i.e., a second device class may have a tamper resistance and/or work factor different from the tamper resistance and/or work factor of the first device class). (p.18, ll.1-5). • Therefore, Applicants disclose digitally signing a second load module (e.g., a video file or a digital image) with a second digital signature different from the first digital signature (i.e., encrypted unique control data), the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class (i.e., encrypted control/usage elements can require the user's data processor to have different security modules in order to use different data objects).

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

(c) distributing the first load module for use by at least one device in the first device class; and	Applicants disclose that a secured data package, for example a digital image (i.e., a first load module) is transferred/distributed to a user for use on the user's data processor having certain required security modules (i.e., distributed for use by at least one device in a first device class). (p.5, ll.17-19; p.20, l.5-p.22, l.12).
(d) distributing the second load module for use by at least one device in the second device class.	Applicants disclose that a secured data package, for example a video film (i.e., a second load module) is transferred/distributed to a user's data processor which must have a different set of security modules, as compared to the example in (c) involving a digital image, in order for the video film to be used (i.e., distributed for use by at least one device in a second device class). (p.5, ll.17-19; p.22, l.13-23). *See* (b) above.

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

Pursuant to 37 C.F.R. §1.607(a)(2), Applicants present the following proposed count 1:

1. A security method comprising:

(a) digitally signing a first load module with a first digital signature designating the first load module for use by a first device class;

(b) digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having a tamper resistance and/or work factor substantially different from the tamper resistance and/or work factor of the first device class;

(c) distributing the first load module for use by at least one device in the first device class; and

(d) distributing the second load module for use by at least one device in the second device class.

Applicants submit that proposed count 1 corresponds to the patentee's claim 1 and to Applicants' claim 54.

The present application was filed on May 27, 1999 as a continuation of U.S. Patent Application No. 09/164,606, filed October 1, 1998, which in turn claimed priority to U.S. Patent Application No. 08/594,811, filed on January 31, 1996, now U.S. Patent No. 5,845,281, which in turn claimed priority to Swedish Application No. 9500355-4, filed on February 1, 1995. The present application is based on the same disclosure as U.S. Patent Application No. 08/594,811, now U.S. Patent No. 5,845,281, which contained the same disclosure as in Swedish Application No. 9500355-4. Thus, Claim 54 is supported by the disclosure of Swedish Application No. 9500355-4 and is entitled to a priority date of February 1, 1995.

The application that matured into U.S. Patent No. 6,292,569 was filed on October 4, 2000, and claimed priority to U.S. Patent Application No. 08/689,754, filed on August 12, 1996, now U.S. Patent No. 6,157,721. Thus, because the present application has a priority date of over 1.5 years prior to the priority date of the patentee, Applicants allege that based upon priority of invention, Applicants are entitled to a judgment relative to the patentee.

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049

35 U.S.C. § 135(b) does not bar this amendment because the amendment is being filed within twelve months of the issuance date of the target patent, September 18, 2001.

CONCLUSION

Accordingly, Applicants respectfully request that an interference be declared between the present Applicants and inventors of the aforementioned patent. If there are any questions, please do not hesitate to call the undersigned at (408) 392-9250.

Express Mail Label No.:

EV 174 799 501US

Respectfully submitted,

#42,406 for

Alan H. MacPherson
Attorney for Applicant(s)
Reg. No. 24,423

LAW OFFICES OF
MACPHERSON KWOK CHEN
& HEID LLP

2402 MICHELSON DRIVE
SUITE 210
IRVINE, CA 92612
(949) 752-7040
FAX (949) 752-7049